Konstruksi Kode Reed-Solomon sebagai Kode Siklik dengan Polinomial Generator

Ryan Pebriansyah Jamal[1,*], Loeky Haryanto[2], Amir Kamal Amir[3]

[1]Jurusan Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Hasanuddin
Jalan Perintis Kemerdekaan, Makassar, Indonesia, Kode Pos 90245

Construction of Reed-Solomon Code as Cyclic Code by Using Polynomial Generator

Ryan Pebriansyah Jamal[1,*], Loeky Haryanto[2], Amir Kamal Amir[3]

[1]Department of Mathematics, Faculty of Mathematics and Natural Sciences, Hasanuddin University
Perintis Kemerdekaan Street, Makassar, Indonesia, Post Code 90245

ABSTRAK

Suatu kode pengoreksi kesalahan adalah himpunan vektor kode yang dirancang untuk mendeteksi dan mengoreksi kesalahan bit di dalam untaian yang diterima atau diakses. Kode siklik adalah salah satu kelas dari kode pengoreksi kesalahan. Kode siklik mempunyai subkelas yang disebut sebagai kode BCH yang mempunyai bentuk khusus yang disebut Kode Reed-Solomon. Kode Reed-Solomon mempunyai kemampuan mengoreksi kesalahan yang tinggi. Pada tulisan ini kode Reed-Solomon dibatasi bekerja pada lapangan hingga (Galois Field) $GF(2^m)$, untuk m bilangan bulat.. Lebih tepatnya, kode Reed-Solomon yang merupakan ideal prima dari $GF(2^m)/\langle x^n - 1\rangle$ dalam tulisan ini dikonstruksi dengan menggunakan sebuah polinom generator $g(x) \in GF(2^m)/\langle x^n - 1\rangle$. Agar bisa mengoreksi t kesalahan bit dan merentang kode Reed-Solomon dengan panjang $n = 2^m - 1$, dimensi $k = n - 2t$, jarak minimum $d_{min} = n - k + 1$ dan memuat q^k vektor kode, polinom generator harus memiliki derajat 2*t*.

Kata Kunci: *kode Reed-Solomon, kode siklik, pengkodean, polinomial generator.*

ABSTRACT

An error-correcting code is a code that is designed to detect and correct bit errors in the received or accessed strings. Cyclic codes belong to a class of error-correcting codes. Cyclic codes include a subclass called BCH codes which in turn include smaller subclass called Reed-Solomon codes. These classes of codes are able to correct many bit errors efficiently. In this work, Reed-Solomon is algebraically constructed over the Galois field $GF(2^m)$, for some positive integer *m*. Precisely, the code is a prime ideal of $GF(2^m)/\langle x^n - 1\rangle$ generated by a polynomial generator $g(x) \in GF(2^m)/\langle x^n - 1\rangle$. In order to be able correcting t bit errors and generating a Reed-Solomon code of length $n = 2^m - 1$, dimension $k = n - 2t$, minimum distance $d_{min} = n - k + 1$ and containing q^k codewords, the polynomial generator must have degree 2*t*.

Keywords: *coding, cyclic codes, polynomial generator, Reed-Solomon codes.*

1. PENDAHULUAN

Perkembangan teknologi telekomunikasi memberikan kemudahan kepada manusia untuk berkomunikasi atau mengirim pesan dari suatu tempat ke tempat yang lain. Dalam pengiriman pesan mungkin terjadi gangguan sehingga pesan yang diterima berbeda dengan pesan yang dikirim. Untuk mengatasinya, pengiriman pesan tidak di dalam bahasa aslinya tetapi terlebih dahulu diubah (dikodekan) ke dalam bentuk vektor kode yang disebut dengan proses pengkodean (*encoding*). Himpunan yang anggotanya vektor kode disebut sebagai kode. Pendefinisian kode ini dilakukan sedemikian sehingga apabila terjadi perubahan beberapa simbol pada vektor kode, maka kesalahan itu bisa dipulihkan lagi oleh dekoder. Sedangkan pengubahan kembali dari vektor biner ke pesan yang berbahasa asli dinamakan pendekodean (*decoding*).

Secara umum, tujuan dari teori pengkodean adalah untuk mengonstruksi suatu kode sehingga dapat mengkodekan suatu pesan dengan cepat, mentransmisi pesan yang sudah dikodekan dengan mudah,

* Penulis koresponden.
Alamat E-mail: ryanpebriansyahjamal@gmail.com

mendekode suatu pesan yang diterima dengan cepat, memaksimalkan informasi yang ditransfer per satuan waktu dan secara maksimal dalam mendeteksi dan mengoreksi kesalahan.

Diantara beberapa jenis kode, dikenal suatu kode yang disebut kode siklik. Kode siklik adalah sebuah kelas dari kode yang sangat penting [7]. Kode siklik menarik dan penting untuk dipelajari karena kaya akan struktur aljabar yang dapat digunakan pada berbagai hal dan mempunyai spesifikasi yang ringkas. Satu dari kelas kode yang sangat penting dari kode siklik diperkenalkan oleh matematikawan R.C. Bose , D.K Ray-Chaudhuri dan A. Hocquenghem pada tahun 1959. Kode ini dikenal sebagai kode BCH [1]. Generalisasi dari kode BCH biner pada kode dalam p^m simbol dengan p adalah bilangan prima dan m suatu bilangan bulat ditemukan oleh Gorenstein dan Zierler [2]. Diantara bentuk kode BCH terdapat subkelas yang sangat penting yang dikenal sebagai kode Reed-Solomon yang diperkenalkan oleh Irving Reed dan Gus Solomon melalui makalahnya dalam *Journal of the Society for Industrial and Applied Mathematics* yang dipublikasikan tahun 1960 dengan judul '*Polynomial Codes over Certain Finite Fields*'.

Dalam dunia aplikasi, kode Reed-Solomon digunakan sebagai pengoreksi kesalahan pada *Compact Disc*, DVD dan yang paling terkenal adalah pengiriman foto-foto dalam eksplorasi planet oleh NASA (*National Aeronautics and Space Administration*) dan ESA (*European Space Agency*) seperti program Mariner yang mengirim serangkaian wahana antarplanet untuk menyelidiki Mars, Venus, dan Merkurius dari tahun 1962 hingga 1973 dan pada saat ekspedisi oleh Voyager 2 dalam melakukan perjalanan ke ke Uranus (1986) dan Neptunus (1989) [8].

Salah satu kelebihan dari kode Reed-Solomon adalah kemampuan mengoreksi kesalahan yang sangat tinggi. Selain itu kode Reed-Solomon juga memiliki algoritma *encoding* dan *decoding* yang efisien. Dalam tulisannya, Wicker dan Bhargava (1994) memaparkan tiga cara untuk mengonstruksi kode Reed-Solomon yaitu dengan aritmatika lapangan hingga (konstruksi orisinil), polinomial generator dan transformasi Fourier. Moon (2011) dalam tulisannya *Introduction to Reed-Solomon Codes* menuliskan ulang pembahasan Wicker dan Bargava secara ringkas dalam bentuk yang lebih terstruktur dan hanya membahas satu aplikasi dari kode Reed-Solomon yaitu pada *Compact Disc*. Konstruksi kode Reed-Solomon dengan polinomial generator adalah metode yang paling sering digunakan saat ini [8].

Dalam tulisan ini yang menjadi masalah yang akan dibahas adalah bagaimana mengonstruksi polinomial generator yang dapat langsung digunakan untuk mengonstruksi kode Reed-Solomon pengoreksi t-kesalahan atas lapangan hingga $GF(2^m)$ dan bagaimana menentukan vektor kode hasil konstruksi kode Reed-Solomon pengoreksi t-kesalahan atas lapangan hingga $GF(2^m)$ dengan polinomial generator.

Dalam tulisan ini penjelasan dari proses untuk mengonstruksi kode Reed-Solomon pengoreksi t-kesalahan dibatasi bekerja pada lapangan hingga $GF(2^m)$ untuk m suatu bilangan bulat, dalam hal ini diberikan contoh untuk $t = 1,2,3$ dan $m = 2,3,4$. Pembatasan dibatasi pada encoding kode Reed-Solomon.

2. BEBERAPA PENGERTIAN DAN NOTASI

2.1. Gelanggang

Sebuah gelanggang R adalah himpunan dengan dua operasi biner $+$ dan $\cdot$, yang memenuhi sifat grup abel terhadap operasi penjumlahan, tertutup terhadap operasi perkalian, dan $a(bc) = (ab)c$ untuk setiap $a, b, c \in R$, serta berlaku hukum distributif. Contoh dari gelanggang adalah $\mathbb{C}$, $\mathbb{R}$, dan $\mathbb{Z}$. Misalkan R adalah sebuah gelanggang dan $I \subset R$ adalah subgelanggang. Maka $I \subset R$ disebut ideal jika $\forall r \in R$ dan $x \in I$ maka $rx \in I$.

1.2. Lapangan Hingga

Gelanggang F disebut lapangan jika F gelanggang komutatif dan F memiliki elemen satuan serta Setiap elemen tak nol di F memiliki invers terhadap operasi perkalian di F. Himpunan bilangan rasional $\mathbb{Q}$ dan himpunan bilangan real $\mathbb{R}$ dengan operasi penjumlahan dan operasi perkalian yang telah dikenal membentuk lapangan. Suatu lapangan yang banyak elemennya berhingga disebut lapangan hingga atau disebut juga sebagai lapangan Galois (Galois Field) diambil dari nama seorang matematikawan Perancis Evariste Galois. $\mathbb{Z}_p = \{0,1,2, \dots, p-1\}$ dengan p adalah bilangan prima adalah lapangan berhingga.

Suatu polinom tak konstan $f(x) \in GF(q)[x]$ dikatakan irreduksi atas lapangan F jika $f(x)$ tak bisa dinyatakan sebagai hasil kali $g(x)h(x)$ antara dua polinom $g(x)$ dan $h(x)$ yang bukan konstan dan berbeda derajatnya dengan f. Polinomial yang koefisien variabel pangkat tertingginya sama dengan 1 (monik) yang irreduksi disebut polinomial prima. Di dalam $\mathbb{Z}[x]$, 3 adalah polinomial derajat nol yang bukan unit (tak

memiliki invers) tetapi di dalam $\mathbb{Q}[x]$, 3 adalah polinom derajat nol yang juga unit, sebab ada $3^{-1} = \frac{1}{3} \in \mathbb{Q}$. Jadi, polinom $f(x) = 3x^2 + 6 = 3(x^2 + 2)$ irreduksi atas $\mathbb{Q}$, tetapi tereduksi atas $\mathbb{Z}$. Salah satu kriteria kereduksian suatu polinom $f(x) \in GF(q)[x]$, jika $\text{der}(f(x)) \leq 3$, maka $f(x)$ irreduksi jika untuk setiap $a \in GF(q)$ berlaku $f(a) \neq 0$.

2.3. Konstruksi Lapangan Hingga

Setiap lapangan hingga $GF(q)$ mempunyai elemen primitif, sedemikian sehingga jika α adalah elemen primitif dari $GF(q)$ maka $GF(q) = \{0, 1, \alpha^1, \alpha^2, \ldots, \alpha^{q-2}\}$. Polinomial primitif $p(x)$ adalah sebuah polinomial prima atas lapangan hingga $GF(q)$ yang digunakan untuk mengonstruksi lapangan perluasan $GF(q)[x]$ modulo $p(x)$. Misalkan diberikan lapangan hingga $GF(q)$ dan lapangan $GF(Q)$ sebagai lapangan perluasan $GF(q)$. Misal α adalah elemen $GF(Q)$. Polinomial prima $f(x)$ dengan derajat terkecil atas lapangan $GF(q)$ dengan $f(\alpha) = 0$ disebut polinomial minimal dari α atas $GF(q)$.

Misalkan $i(x) \in GF(p)[x]$ adalah polinomial irreduksi dan berderajat $n > 1$. Terdapat sebuah lapangan terkecil E_α yang memuat α. Lapangan E_α memiliki karakteristik $p > 0$ sehingga $GF(p) \subseteq E_\alpha$. Langkah-langkah konstruksi lapangan perluasan E_α, yang selanjutnya dinamakan lapangan Galois $GF(p^m)$ sebagai berikut.

1. Pilih lapangan hingga $F = GF(p)$, untuk suatu bilangan prima p.
2. Pilih polinomial irreduksi $i(x) \in GF(p)[x]$ dengan $\text{der}(i) = n > 1$.
3. Dengan Algoritma Hasil Bagi Euclid, dikonstruksi lapangan terkecil $E_\alpha = GF(q)$, dengan $q = p^m$ sebagai himpunan yang terdiri atas q *b*entuk sisa hasil pembagian $f(\alpha)$ oleh $i(\alpha)$, di mana $f(x) \in GF(p)[x]$.
4. Algoritma pembagian Euclid diimplementasikan melalui kesamaan $i(\alpha) = 0$. Hasil kali dan hasil tambah unsur-unsur $E_\alpha = GF(q)$ juga diperoleh dari kesamaan $i(\alpha) = 0$.

2.4. Kode Linier

Diberikan ruang vektor $V(n, 2)$ atas lapangan $GF(2) = \{0, 1\}$, yaitu himpunan vektor-vektor biner $\boldsymbol{v}$ dengan panjang n yang dilengkapi operator tambah (modulo 2) dan perkalian antara skalar $c \in F_2 = \{0, 1\}$ dengan $\boldsymbol{v} \in V(n, 2)$ yang memenuhi sifat: Untuk setiap $\boldsymbol{v} \in V(n, 2)$ berlaku $(0)\boldsymbol{v} = \boldsymbol{0}$ dan $(1)\boldsymbol{v} = \boldsymbol{v}$. Himpunan bagian $C \subseteq V(n, 2)$ yang tidak kosong adalah kode linier jika untuk setiap $\boldsymbol{u}, \boldsymbol{v} \in C$ berlaku $\boldsymbol{u} + \boldsymbol{v} \in C$ dan $a\boldsymbol{u} \in C$, $a \in GF(2)$. Setiap unsur $\boldsymbol{c} \in C$ disebut vektor kode. Contoh dari kode linier adalah C_1 = {000, 011, 101, 110} sedangkan C_2 = {101, 111, 011} bukan kode linier karena 101 + 111 = 010 bukan elemen C_2.

Jarak Hamming antara dua vektor $\boldsymbol{u}, \boldsymbol{v} \in V(n, 2)$ dinyatakan dengan simbol $d(\boldsymbol{u}, \boldsymbol{v})$ dan didefinisikan sebagai banyak bit yang berbeda di antara komponen-komponen $\boldsymbol{u}$ dan $\boldsymbol{v}$. Jika C adalah sebuah kode, maka jarak minimal kode C dilambangkan dengan $d(C)$ dan didefinisikan sebagai $d(C) = min\{d(\boldsymbol{u}, \boldsymbol{v}) | \boldsymbol{u}, \boldsymbol{v} \in C \; dan \; \boldsymbol{u} \neq \boldsymbol{v}\}$. Jika jarak minimal dari kode *C* adalah *d*, maka disebut kode [n, k, d].

Sebuah matriks $k \times n$ yang barisnya membentuk basis untuk kode linier $C[n, k]$ disebut matriks perentang (generator matrix) untuk kode C. Sebagai contoh matriks perentang dari kode $C_1 = \{000, 011, 101, 110\}$ adalah $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$.

2.5. Pengkodean *(Encoding)* dengan Kode Linier

Proses pengubahan informasi atau pesan ke dalam bentuk vektor biner disebut sebagai pengkodean (*encoding*). Misalkan C adalah kode linier $[n, k]$ atas $GF(q)$ dengan matriks generator G maka C memiliki q^k vektor kode. Encoding dari sebuah pesan $u = (u_1, \ldots, u_k) \in V(k, 2)$ menjadi kode di dalam C dilakukan dengan cara $u.G = \sum_{i=1}^{k} u_i \, r_i$ dimana $(r_1, \ldots, r_k)$ adalah baris pada matriks generator *G*.
Sebuah pesan $\boldsymbol{u}$ = *(u₁, u₂, u₃, u₄)* dikodekan menjadi $u.G = \sum_{i=1}^{k} u_i \, r_i$.

2.6. Kode Siklik

Sebuah kode C dikatakan siklik jika untuk setiap vektor $c = (c_1, c_2, \ldots, c_{n-1}, c_n) \in C$ maka $(c_n, c_1, c_2, \ldots, c_{n-1}) \in C$. Contohnya, jika (1,1,0,1) adalah elemen sebuah kode siklik, maka (1,1,1,0) juga termuat dalam kode siklik tersebut. Dengan demikian, operasi pergeseran siklis memetakan kode C ke dirinya sendiri. Sehingga jika diberikan suatu matriks G yang merentang kode siklik, untuk menentukan

semua vektor kode dari kode sikliknya dapat dilakukan dengan melakukan pergeseran secara siklik pada vektor perentangnya.

2.7. Kode BCH dan Kode Reed-Solomon

Salah satu kelas dari kode siklik adalah kode BCH yang ditemukan oleh R.C. Bose dan D. K. Ray-Chaudhuri pada tahun 1959. Bentuk khusus dari kode BCH adalah Kode Reed-Solomon yang juga bekerja atas lapangan hingga. Kode Reed-Solomon sendiri ditemukan oleh Irving Reed dan Gus Solomon pada tahun 1959. Unsur-unsur dari kode BCH dan Reed-Solomon lebih mudah ditulis sebagai polinomial $c(x) = c_0 + c_1x + \cdots + c_{k-1}x^{k-1}$. Dengan menggunakan polinomial generator $g(x) \in C$, setiap vektor kode Reed-Solomon berbentuk $c(x) = m(x)g(x), \forall m(x) \in GF(q^k)[x]/\langle x^{n-1}\rangle$.

Kode Reed-Solomon adalah sebuah ideal C dari gelanggang hasil bagi $GF(q^k)[x]/\langle x^{n-1}\rangle$ yaitu $C \subseteq GF(q^k)[x]/\langle x^{n-1}\rangle$, artinya $\forall f(x) \in C$ berlaku $f(x)r(x) \in C, \forall r(x) \in GF(q^k)[x]/\langle x^{n-1}\rangle$.

3. HASIL DAN PEMBAHASAN

3.1. Kode Siklik sebagai Ideal

Definisi 3.1 *Suatu kode linier C atas lapangan $GF(2^m)$ disebut sebagai sebuah kode siklik dengan panjang n jika untuk setiap vektor kode $\boldsymbol{c} = (c_0, c_1, c_2, \dots, c_{k-2}, c_{n-1}) \in C$ maka vektor $\boldsymbol{c}' = (c_{n-1}, c_0, c_1, \dots, c_{n-3}, c_{n-2})$ yang diperoleh dari pergeseran siklik kordinat $i \mapsto i + 1$ mod (n) juga berada di dalam C.*

Diberikan kode siklik C dan fungsi satu-satu yang memetakan vektor kode $\boldsymbol{c} = (c_0, c_1, \dots, c_i, \dots, c_{n-2}, c_{n-1}) \in C$ ke vektor polinomial $c(x) = c_0 + c_1x + \cdots + c_ix^i + \cdots + c_{n-1}x^{n-1} \in GF(2^m)[x]/\langle x^n - 1\rangle$. Daerah hasil (*range*) dari pemetaan ini merupakan ideal yang merupakan penyajian kode siklik C sebagai himpunan polinomial.

Teorema 3.1 [5]. *Sebuah kode linier C adalah siklik jika dan hanya jika C adalah sebuah ideal dari $GF(2^m)[x]/\langle x^n - 1\rangle$.*

Bukti :

(i) Jika C adalah ideal dari $GF(2^m)[x]/\langle x^n - 1\rangle$ dan $c(x) = c_0 + c_1x + \cdots + c_ix^i + \cdots + c_{n-1}x^{n-1}$ adalah sebuah vektor kode, maka $xc(x) = x(c_0 + c_1x + \cdots + c_ix^i + \cdots + c_{n-1}x^{n-1}) = c_{n-1} + c_0x + c_1x^2 + c_2x^3 + \cdots + c_{n-2}x^{n-1}\ mod\ (x^n - 1) \in C$.

(ii) Sebaliknya, jika C adalah kode siklik, maka untuk setiap vektor kode $c(x)$, vektor kode $xc(x)$ juga berada di dalam C. Dengan demikian $x^ic(x)$ juga berada di dalam C untuk setiap i. Karena C adalah kode linier, $a(x)c(x)$ juga berada di dalam C untuk setiap polinomial $a(x)$. Oleh karena itu, C adalah sebuah ideal.

3.2. Konstruksi Kode Siklik

Misalkan C adalah kode siklik yang panjangnya n atas sebuah lapangan hingga $GF(q)$. Untuk setiap vektor kode $(c_0, c_1, \dots, c_{n-1}) \in C$ mewakili polinomial $c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ dalam $GF(q)[x]$. Misal $g(x)$ mempunyai derajat terkecil diantara semua polinomial tak nol yang diperoleh dari C. Polinomial $g(x)$ disebut **polinomial generator** (*generating polynomial*) untuk C. Maka, $g(x)$ ditentukan secara tunggal oleh C dan merupakan pembagi dari $x^n - 1$. C adalah himpunan dari koefisien dari polinomial $g(x)f(x)$ dengan $der(f(x)) \leq n - 1 - der(g(x))$. Tulis $x^n - 1 = g(x)h(x)$. Maka $c(x) \in GF(q)[x]/\langle x^n - 1\rangle$ berkorespondensi pada sebuah elemen dari C jika dan hanya jika $h(x)c(x) \equiv 0\ mod\ (x^n - 1)$. [8]

Misal $g(x) = a_0 + a_1x + \cdots + a_{k-1}x^{m-1} + x^m$. Setiap elemen dari C berkorespondensi pada sebuah polinomial dari bentuk $g(x)f(x)$, dengan derajat $\deg(f(x)) \leq n - 1 - m$. Ini artinya setiap $f(x)$ adalah sebuah kombinasi linier dari monomial $1, x, x^2, x^3, \dots, x^{n-1-m}$. Sehingga vektor kode dari C adalah kombinasi linier dari vektor kode yang berkorespondensi pada polinomial

$$g(x), g(x)x, g(x)x^2, g(x)x^3, \dots, g(x)x^{n-1-m}.$$

yang juga merupakan vektor-vektor

$$(a_0, \dots, a_m, 0, 0, \dots), (0, a_0, \dots, a_m, 0, \dots), \dots, (0, \dots, 0, a_0, \dots, a_m).$$

Dengan demikian matriks generator untuk C diberikan oleh

$$G = \begin{pmatrix} a_0 & a_1 & \dots & a_m & 0 & 0 & \dots \\ 0 & a_0 & a_1 & \dots & a_m & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & a_0 & a_1 & \dots & a_m \end{pmatrix}.$$

Untuk mengonstruksi suatu kode siklik dapat dilakukan dengan melihat dari matriks generatornya atau secara aljabar dari polinomial generatornya.

Contoh 3.1. Misalkan diberikan matriks biner yang membangun kode $C[7,3]$ sebagai berikut

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Dalam hal ini, pergeseran siklis dari baris pertama memberikan semua vektor kode tak nol dari kode C.

$C = \{(0,0,0,0,0,0,0), (1,1,1,0,1,0,0), (0,1,1,1,0,1,0), (0,0,1,1,1,0,1),$
$(1,0,0,1,1,1,0), (0,1,0,0,1,1,1), (1,0,1,0,0,1,1), (1,1,0,1,0,0,1)\}$.

Jarak minimum dari kode adalah 4, jadi kode siklik $C[7,3,4]$.

Secara aljabar, dipilih polinomial generator yang membangun kode $C[7,3]$ yaitu polinomial irreduksi $g(x)$ yang berderajat 4 yang membagi $x^7 - 1$. Misal $g(x) = 1 + x + x^2 + x^4$. Perhatikan hasil kali antara $g(x)$ dan $f(x)$

$$g(x)f(x) = a_0 + a_1x + \cdots + a_6x^6,$$

dengan $f(x)$ adalah polinomial yang derajatnya kurang dari 3. Tulis koefisien polinomial dari hasil perkalian sebagai sebuah vektor kode.

$g(x) \cdot 0 = 0 + 0x + 0x^3 + 0x^4 = 0 \leftrightarrow (0,0,0,0,0,0,0)$
$g(x) \cdot 1 = 1 + x + x^2 + x^4 \leftrightarrow (1,1,1,0,1,0,0)$
$g(x) \cdot x = x + x^2 + x^3 + x^5 \leftrightarrow (0,1,1,1,0,1,0)$
$g(x) \cdot (1 + x) = 1 + x^3 + x^4 + x^5 \leftrightarrow (1,0,0,1,1,1,0)$
$g(x) \cdot x^2 = x^2 + x^3 + x^4 + x^6 \leftrightarrow (0,0,1,1,1,0,1)$
$g(x) \cdot (1 + x^2) = 1 + x + x^3 + x^6 \leftrightarrow (1,1,0,1,0,0,1)$
$g(x) \cdot (x + x^2) = x + x^4 + x^5 + x^6 \leftrightarrow (0,1,0,0,1,1,1)$
$g(x) \cdot (1 + x + x^2) = 1 + x^2 + x^5 + x^6 \leftrightarrow (1,0,1,0,0,1,1)$.

Dengan demikian, diperoleh kode siklik

$C = \{(0,0,0,0,0,0,0), (1,0,1,1,1,0,0), (0,1,0,1,1,1,0), (0,0,1,0,1,1,1),$
$(1,0,0,1,0,1,1), (1,1,0,0,1,0,1), (1,1,1,0,0,1,0), (0,1,1,1,0,0,1)\}$.

3.3 Kode BCH

Kode BCH adalah sebuah kode dari kelas kode siklik yang memiliki algoritma pendekodean (*decoding*) yang baik.

Definisi 3.2. *Sebuah kode siklik dengan panjang n atas lapangan GF(q) dikatakan sebagai **kode BCH** dengan jarak d jika polinomial generatornya $g(x)$ adalah kelipatan persekutuan terkecil dari polinomial minimal dari $\alpha^l, \alpha^{l+1}, \dots, \alpha^{l+q-2}$ untuk suatu l, dengan α adalah akar primitif. Biasanya diambil $l = 1$ yang disebut sebagai narrow-sense dari kode BCH.*

Untuk suatu bilangan bulat positif m dan $t < 2^{m-1}$, terdapat sebuah kode BCH dengan panjang vektor kode $n = 2^m - 1$, dan jarak minimum $d \geq 2t + 1$ serta berlaku $n - k \leq mt$. Kode ini disebut kode BCH biner pengoreksi t-kesalahan. Polinomial generator untuk mengonstruksi kode ini dispesifikasikan dalam bentuk akar-akar dari lapangan hingga $GF(2^m)$.

Misal α adalah elemen primitif dari lapangan $GF(2^m)$. Polinomial generator $g(x)$ dari kode BCH pengoreksi t-kesalahan dengan panjang vektor kode $n = 2^m - 1$ adalah polinomial minimal atas $GF(q)$ yang mempunyai $\alpha, \alpha^2, \alpha^3, \dots, \alpha^{2t}$ sebagai akar-akarnya sedemikian sehingga $g(\alpha^j) = 0, 1 \leq j \leq 2t$.

Kode BCH yang didefiniskan diatas disebut sebagai **kode BCH primitif**.

3.4. Kode Reed-Solomon

Kode Reed-Solomon ditemukan oleh Irving Reed dan Gus Solomon, yang kemudian disajikan dalam makalah *"Polynomial Codes over Certain Finite Fields"* dalam *Journal of the Society for Industrial and Applied Mathematics* pada tahun 1959. Sejak saat itu, kode Reed-Solomon telah menjadi kontributor dalam revolusi telekomunikasi yang berlangsung dari pertengahan abad ke-20 [1]. Kode Reed-Solomon adalah kode siklik non biner dengan simbol kode dari lapangan Galois.

Definisi 3.3. *Kode Reed-Solomon (RS code) pengoreksi t-kesalahan adalah sebuah kode BCH primitif dengan panjang $n = q - 1$ atas lapangan $GF(q)$.*

Polinomial generator dari kode ini mempunyai bentuk $g(x) = \prod_{i=1}^{2t}(x - \alpha^i)$ dengan α adalah unsur primitif dalam $GF(q)$. Kode Reed-Solomon mempunyai dimensi $k = n - d + 1$, yang disebut sebagai *Maximum Distance Separable (MDS).* Untuk setiap bilangan bulat positif $t \leq 2^m - 1$, terdapat sebuah kode Reed-Solomon pengoreksi t-kesalahan dengan simbol dari $GF(2^m)$, dengan parameter-parameter $n = 2^m - 1$, $k = n - 2t$ dan $d_{min} = 2t + 1 = n - k + 1$. Sehingga jika diketahui terjadi t koordinat kesalahan dari n koordinat pada kode yang dterima. Kode Reed-Solomon dapat mengoreksi hingga $t = \left\lfloor \frac{n-k+1}{2} \right\rfloor$ kesalahan.

Contoh 3.2. Misalkan lapangan hingga $GF(p^m)$, dengan $p = 2$ dan $m = 8$ sehingga panjang vektor kode $n = 2^8 - 1 = 255$. Diketahui $t = 16$ maka dimensi dari kode adalah $k = n - 2t = 223$ dan $d_{min} = n - k + 1 = 255 - 223 + 1 = 33$. Jadi, kode yang terbentuk adalah kode Reed-Solomon (252,223,33). Kode ini juga dikenal sebagai kode standar yang digunakan NASA pada satelit komunikasi.

3.5. Konstruksi Kode Reed Solomon dengan Polinomial Generator

Metode polinomial generator untuk mengonstruksi sebuah kode Reed-Solomon yang mengoreksi t-kesalahan adalah pendekatan yang paling sering digunakan saat ini [2]. Untuk mengonstruksi sebuah kode Reed-Solomon dengan panjang $q - 1$ atas lapangan $GF(q)$ dengan $q = p^m$, ambil sebuah elemen primitif $\alpha \in GF(q)$, kemudian konstruksi polinomial generator $g(x)$ dengan akar-akarnya $\alpha, \alpha^2, \ldots, \alpha^{2t}$:

$$g(x) = \prod_{i=1}^{2t}(x - \alpha^i) = (x - \alpha)(x - \alpha^2) \ldots (x - \alpha^{2t}) = g_0 + g_1 x + g_2 x^2 + \cdots + g_{2t-1} x^{2t-1} + g_{2t} x^{2t}$$

dengan $g_i \in GF(q)$.

Dari bentuk polinomial generatornya diketahui bahwa derajatnya adalah $2t$. Koefisien dari polinomial generator berbentuk polinomial dengan variabel α yang kemudian diubah kedalam representasi perpangkatan dari α. Polinomial generator dengan koefisien berbentuk $\alpha^i \in GF(2^m)$ dapat langsung digunakan untuk mengonstruksi kode Reed-Solomon pengoreksi t-kesalahan.

Contoh 3.3. Konstruksi kode Reed-Solomon pengoreksi 1-kesalahan atas lapangan hingga $GF(2^3)$.
Misalkan lapangan $GF(2^3)$ dengan polinomial primitif $p(x) = 1 + x + x^3$. Misalkan α adalah akar dari $p(x)$, sehingga $p(\alpha) = 1 + \alpha + \alpha^3 = 0 \rightarrow \alpha^3 = \alpha + 1$.

Jika akan dikonstruksi sebuah kode Reed-Solomon pengoreksi 1-kesalahan maka polinomial generatornya adalah $g(x) = (x - \alpha)(x - \alpha^2) = \alpha^3 + (\alpha + \alpha^2)x + x^2$. Koefisien dari polinomial generator dapat dinyatakan dalam representasi bentuk perpangkatan dari α dari bentuk polinomialnya dengan menggunakan reduksi modulo $p(\alpha) = 1 + \alpha + \alpha^3 = 0 \rightarrow \alpha^3 = 1 + \alpha$.

$$GF(2^3) = \{0, 1, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$$

Tabel 1. Representasi elemen dari $GF(2^3)$ dengan α sebagai elemen primitif

α^i	**Representasi Polinomial**
α^0	1
α^1	α
α^2	α^2
α^3	$1 + \alpha$
α^4	$(\alpha^3)\alpha = (1 + \alpha)\alpha = \alpha + \alpha^2$
α^5	$(\alpha^3)\alpha^2 = (1 + \alpha)\alpha^2 = \alpha^2 + \alpha^3 = \alpha^2 + (1 + \alpha) = 1 + \alpha + \alpha^2$
α^6	$(\alpha^3)^2 = (1 + \alpha)^2 = 1 + \alpha + \alpha + \alpha^2 = 1 + \alpha^2$

Untuk koefisien x
$\alpha + \alpha^2 = \alpha^4$.

Sehingga diperoleh bentuk polinomial generatornya adalah $g(x) = \alpha^3 + \alpha^4 x + x^2$.

Polinomial generator $g(x)$ akan membangun sebuah kode Reed-Solomon pengoreksi 1-kesalahan dengan parameter sebagai berikut

Panjang vektor kode $n = 2^m - 1 = 2^3 - 1 = 7$; dimensi $k = n - 2t = 7 - 2(1) = 5$;

jarak minimum $d_{min} = n - k + 1 = 7 - 5 + 1 = 3$.

Jumlah vektor kodenya adalah $q^k = 8^5 = 512$ vektor kode.

Untuk menentukan semua vektor kode dari Kode Reed-Solomon [7,5,3] atas lapangan $GF(2^3)$ dapat dilakukan dengan cara mengalikan polinomial $m(x)$ yang berderajat $\text{der}(m(x) \leq n-1-der(g(x)) = 7-1-2 = 4$ atas lapangan $GF(2^3)$

$$m(x) = m_0 + \cdots + m_4x^4, m_i \in GF(2^3) = \{0,1,\alpha,\alpha^2,\ldots,\alpha^6\}, i = 0,1,\ldots,4$$

dengan polinomial generator $g(x) = \alpha^3 + \alpha^4x + x^2$ sehingga diperoleh polinomial $c(x) = c_0 + c_1x + \cdots + c_6x^6, c_i \in GF(2^3) = \{0,1,\alpha,\alpha^2,\ldots,\alpha^6\}, i = 0,1,\ldots 6$.

Polinomial $c(x)$ akan berkorespondensi dengan vektor kode yang panjangnya 7 atas lapangan hingga $GF(2^3) = \{0,1,\alpha,\alpha^2,\ldots,\alpha^6\}$.

Misalkan $m(x) = \alpha x$ akan memberikan vektor kode $c(x) = m(x)g(x) = (\alpha x)(\alpha^3 + \alpha^4x + x^2) = \alpha^4x + \alpha^5x^2 + \alpha x^3$ yang berkorespondensi dengan vektor kode $c = (0, \alpha^4, \alpha^5, \alpha, 0,0,0)$

Vektor kode c dapat dinyatakan atas lapangan $GF(2)$ sebagai bentuk biner dengan terlebih dahulu mengganti representasi perpangkatan α dengan representasi polinomialnya menggunakan reduksi modulo $p(\alpha) = \alpha^3 + \alpha + 1$ yang dapat dilihat pada **Tabel 1**.

$$c = (0, \alpha + \alpha^2, 1 + \alpha + \alpha^2, \alpha, 0,0,0).$$

Kemudian setiap koefisien dari representasi polinomial tersebut merupakan bit biner yang mewakilinya. Misalnya α bersesuaian dengan (010) dan $\alpha + \alpha^2$ bersesuaian dengan (011). Sehingga,

$$c = (0, \alpha + \alpha^2, 1 + \alpha + \alpha^2, \alpha, 0,0,0) \rightarrow c = (000011111010000000000).$$

Contoh 3.4. Konstruksi kode Reed-Solomon pengoreksi 2-kesalahan atas lapangan hingga $GF(2^3)$.
Misalkan lapangan $GF(2^3)$ dengan polinomial primitif $p(x) = 1 + x + x^3$. Misalkan α adalah akar dari $p(x)$, sehingga $p(\alpha) = 1+\alpha + \alpha^3 = 0 \rightarrow \alpha^3 = \alpha + 1$.

Jika akan dikonstruksi sebuah kode Reed-Solomon pengoreksi 2-kesalahan maka polinomial generatornya adalah

$$g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4) = (x^2 - (\alpha + \alpha^2)x + \alpha^3)(x^2 - (\alpha^3+\alpha^4)x + \alpha^7)$$
$$= \alpha^{10} + (\alpha^6 + \alpha^7 + \alpha^8 + \alpha^9)x + (\alpha^3+\alpha^4 + \alpha^6 + \alpha^7)x^2 + (\alpha + \alpha^2 + \alpha^3+\alpha^4)x^3 + x^4.$$

Koefisien dari polinomial generator dapat dinyatakan dalam representasi bentuk perpangkatan dari α dari bentuk polinomialnya dengan menggunakan reduksi modulo $p(\alpha) = 1 + \alpha + \alpha^3 = 0 \rightarrow \alpha^3 = 1 + \alpha$.

$$GF(2^3) = \{0,1,\alpha^1,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6\}$$

Untuk α^{10}

$\alpha^{10} = (\alpha^3)^3\alpha = \alpha^2\alpha = \alpha^3$.

Untuk koefisien x

$$\alpha^6 + \alpha^7 + \alpha^8 + \alpha^9 = (\alpha^3)^2 + (\alpha^3)^2\alpha + (\alpha^3)^2\alpha^2 + (\alpha^3)^3$$
$$= (1 + \alpha^2) + (1 + \alpha^2)\alpha + (1 + \alpha^2)\alpha^2 + (1 + \alpha + \alpha^2 + \alpha^2)$$
$$= (1 + \alpha^2) + (\alpha + \alpha^3) + (\alpha^2 + \alpha^4) + (1 + \alpha + \alpha^2 + \alpha^3)$$
$$= 1 + 1 + \alpha + \alpha + \alpha^2 + \alpha^2 + \alpha^2 + \alpha^3 + \alpha^3 + \alpha^4$$
$$= \alpha^2 + (\alpha + \alpha^2) = \alpha + \alpha^2 + \alpha^2 = \alpha.$$

Untuk koefisien x^2

$$\alpha^3+\alpha^4 + \alpha^6 + \alpha^7 = \alpha^3+(\alpha^3)\alpha + (\alpha^3)^2 + (\alpha^3)^2\alpha = (1 + \alpha) + (1 + \alpha)\alpha + (1 + \alpha)^2 + (1 + \alpha)^2\alpha$$
$$= 1 + \alpha + \alpha + \alpha^2 + (1 + \alpha^2) + (1 + \alpha^2)\alpha = 1 + 1 + \alpha + \alpha + \alpha^2 + \alpha^2 + (\alpha + \alpha^3)$$
$$= \alpha + \alpha^3 = \alpha + (1 + \alpha) = 1 + \alpha + \alpha = 1.$$

Untuk koefisien x^3

$$\alpha + \alpha^2 + \alpha^3+ \alpha^4 = \alpha + \alpha^2 + \alpha^3 + (\alpha^3)\alpha = \alpha + \alpha^2 + (1 + \alpha) + (1 + \alpha)\alpha$$
$$= \alpha + \alpha^2 + 1 + \alpha + \alpha + \alpha^2 = 1 + \alpha + \alpha + \alpha + \alpha^2 + \alpha^2 = \alpha^3.$$

Sehingga diperoleh bentuk polinomial generatornya adalah $g(x) = \alpha^3 + \alpha x + x^2 + \alpha^3x^3 + x^4$.

Polinomial generator $g(x)$ akan membangun sebuah kode Reed-Solomon pengoreksi 2-kesalahan dengan parameter sebagai berikut

Panjang vektor kode $n = 2^m - 1 = 2^3 - 1 = 7$; dimensi $k = n - 2t = 7 - 2(2) = 3$;

jarak minimum $d_{min} = n - k + 1 = 7 - 3 + 1 = 5$.

Jumlah vektor kodenya adalah $q^k = 8^3 = 512$ vektor kode.

Untuk menentukan semua vektor kode dari Kode Reed-Solomon [7,3,5] atas lapangan $GF(2^3)$ dapat dilakukan dengan cara mengalikan polinomial $m(x)$ yang berderajat $\text{der}(m(x) \leq n-1-der(g(x)) = 7-1-4 = 2$ atas lapangan $GF(2^3)$

$$m(x) = m_0 + m_1x + m_2x^2, m_i \in GF(2^3) = \{0,1,\alpha,\alpha^2,\dots,\alpha^6\}, i = 0,1,2$$

dengan polinomial generator $g(x) = \alpha^3 + \alpha x + x^2 + \alpha^3x^3 + x^4$ sehingga diperoleh polinomial $c(x) = c_0 + c_1x + \cdots + c_6x^6, c_i \in GF(2^3) = \{0,1,\alpha,\alpha^2,\dots,\alpha^6\}, i = 0,1,\dots 6$.

Polinomial $c(x)$ akan berkorespondensi dengan vektor kode yang panjangnya 7 atas lapangan hingga $GF(2^3) = \{0,1,\alpha,\alpha^2,\dots,\alpha^6\}$.

Misalkan $m(x) = \alpha x$ akan memberikan vektor kode $c(x) = m(x)g(x) = (\alpha x)(\alpha^3 + \alpha x + x^2 + \alpha^3x^3 + x^4) = \alpha^4x + \alpha^2x^2 + \alpha x^3 + \alpha^4x^4 + \alpha x^5$ yang berkorespondensi dengan vektor kode $c = (0,\alpha^4,\alpha^2,\alpha,\alpha^4,\alpha,0)$.

Vektor kode c dapat dinyatakan atas lapangan $GF(2)$ sebagai bentuk biner dengan terlebih dahulu mengganti representasi perpangkatan α dengan representasi polinomialnya menggunakan reduksi modulo $p(\alpha) = \alpha^3 + \alpha + 1$ yang dapat dilihat pada **Tabel 1**.

$$c = (0,\alpha+\alpha^2,\alpha^2,\alpha,\alpha+\alpha^2,\alpha,0).$$

Kemudian setiap koefisien dari representasi polinomial tersebut merupakan bit biner yang mewakilinya. Misalnya α bersesuaian dengan (010) dan $\alpha + \alpha^2$ bersesuaian dengan (011). Sehingga,

$$c = (0,\alpha+\alpha^2,\alpha^2,\alpha,\alpha+\alpha^2,\alpha,0) \rightarrow c = (000011001010011010000).$$

4. KESIMPULAN

Berdasarkan hasil yang didapatkan, maka dapat disimpulkan:

1. Polinomial generator $g(x)$ yang dapat langsung digunakan untuk mengonstruksi kode Reed-Solomon pengoreksi t-kesalahan atas lapangan hingga $GF(2^m)$ dikonstruksi dari bentuk umum
   $g(x) = \prod_{i=1}^{2t}(x-\alpha^i) = (x-\alpha)(x-\alpha^2)\dots(x-\alpha^{2t}) = g_0 + g_1x + \cdots + g_{2t}x^{2t}$.
   Koefisien polinomial generator g_i untuk $i = 0,1,2,\dots,2t$ berbentuk polinomial dengan variabel α, unsur primitif dalam $\text{GF}(2^m)$. Kemudian dilakukan reduksi modulo polinomial primitif $p(\alpha)$ sehingga menjadi bentuk representasi perpangkatan dari α yang merupakan elemen dari lapangan hingga $GF(2^m) = \{0,1,\alpha,\alpha^2,\dots,\alpha^{2t}\}$.
2. Hasil konstruksi kode Reed-Solomon $[n,k,d]$ berupa himpunan $(2^m)^k$ vektor kode $(c_0,c_1,\dots,c_{n-1})$ dengan panjang $n = 2^m - 1$ diperoleh dari koefisien polinomial
   $c(x) = m(x)g(x) = (m_0 + m_1x + \cdots + m_{n-1-2t}x^{n-1-2t})(g_0 + g_1x + \cdots + g_{2t}x^{2t})$
   $= c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$, dengan $c_i \in GF(2^m) = \{0,1,\alpha,\alpha^2,\dots,\alpha^{2^m-2}\}$ $(i = 0,1,\dots,n-1)$ dan $\text{der}(m(x) \leq n-1-der(g(x))$.

REFERENSI

[1] Betten, Anton dkk. (2006). *Error-Correcting Linear Codes*. Jerman : Springer.

[2] Blahut, Richard E. (2003). *Algebraic Codes for Data Transmission.* Inggris : Cambridge University Press.

[3] Haryanto, Loeky dan Amir Kamal Amir. (2012). *Aljabar Linier Lanjut I*. Makassar : Universitas Hasanuddin.

[4] Huffman, Cary dan Vera Pless. (2003). *Fundamentals of Error-Correcting Codes*. New York : Cambridge University Press.

[5] Lint, J.H. Van. (1999). *Introduction to Coding Theory*. Jerman : Springer.

[6] Moon, Yo Sup. (2011). *Paper : Introduction to Reed-Solomon Codes*. Amerika Serikat : Departments of Mathematics Harvard University.

[7] Skorobogatov. *M2P4 Rings and Fields*. Inggris : Mathematics Imperial College London.

[8] Trape, Wade dan Lawrence C. Washington. (2002). *Introduction to Criptography with Coding Theory*. Amerika Serikat : Prentice Hall.

[9] Wicker, Stephen B. dan Vijhay K. Bargava. (1994). *An Introduction to Reed-Solomon Codes in Reed Solomon Codes and Their Aplications.* New York : IEEE Press.